PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-196081

(43)Date of publication of application : 21.07.1999

(51)Int.Cl. H04L 9/08
G09C 1/00
H04L 9/14

(21)Application number : 09-368942

(22)Date of filing : 26.12.1997

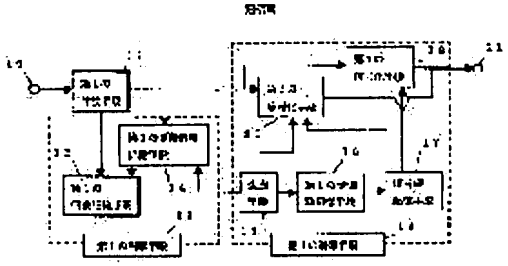
(71)Applicant : KODO IDO TSUSHIN SECURITY GIJUTSU KENKYUSHO:KK

(72)Inventor : ANZAI JUN

(54) CIPHER COMMUNICATION EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To delivery an updated key which is simple in security in the cipher communication equipment where a common (secret) key block cipher is applied to cipher communication and cipher key delivery.



SOLUTION: When a key is updated, a transmission station uses a spare key as a new cipher key, a spare key generated by a generating means 15 is used as a new spare key, the spare key is ciphered by the cipher key and transmitted, then transmission data are ciphered by the cipher key and the result is transmitted. In a reception station, the spare key is used as a new decoding key, the received ciphering key is decoded as a new spare key, and then the received ciphered data are decoded. The same key is used for the cipher communication and key delivery in prescribed security by always preparing the spare key to be updated periodically. Since the key to be used for key delivery is always unused, security is high and the labor and time for managing the delivery key (generation and update) is omitted. Furthermore, it is not required to decide previously a timing of updating the key between the transmission station and the reception station by deciding the timing of updating the key, depending on the spare key and a plain text and the timing of updating the key is at random, then information for facilitating

decoding is hardly specified by a wiretapper.

LEGAL STATUS

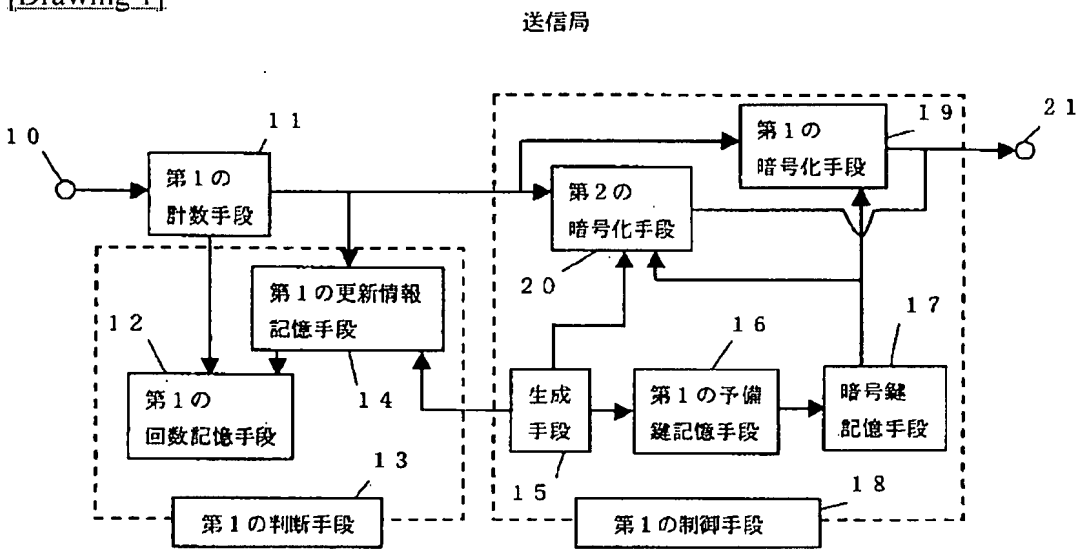
[Date of request for examination]	30.03.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3195288
[Date of registration]	01.06.2001
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	01.06.2004

* NOTICES *

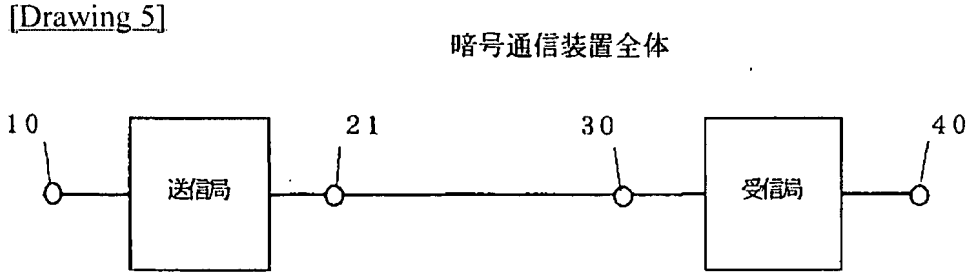
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

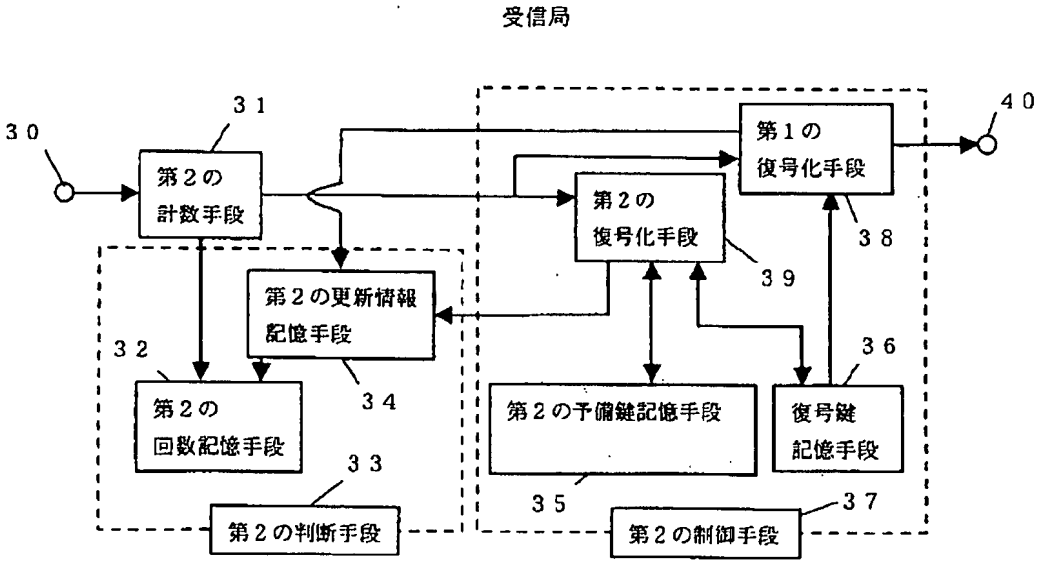
[Drawing 1]



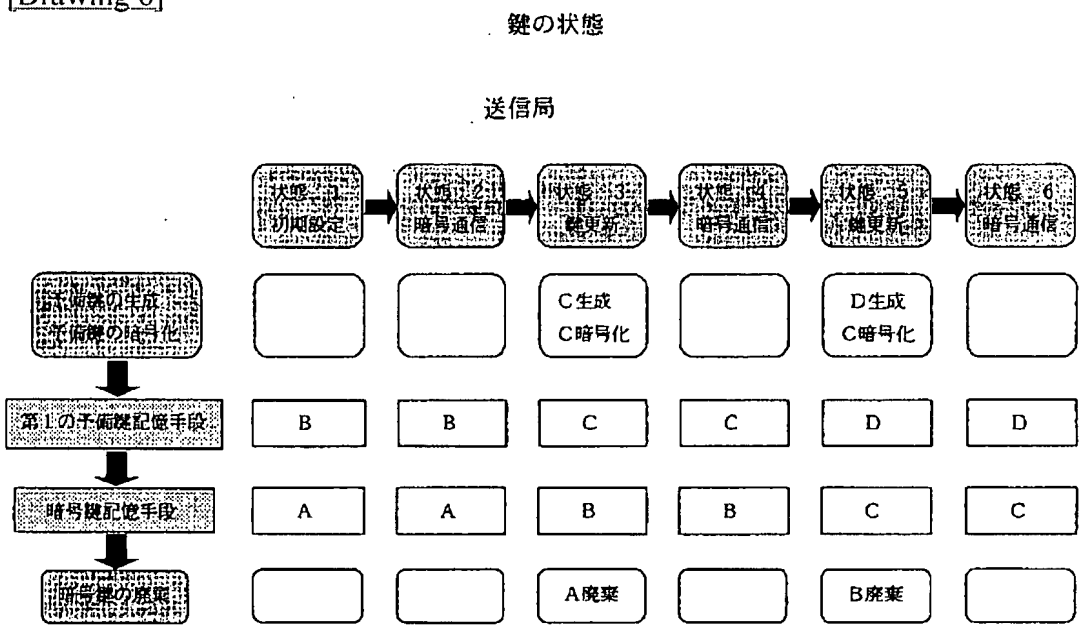
[Drawing 5]



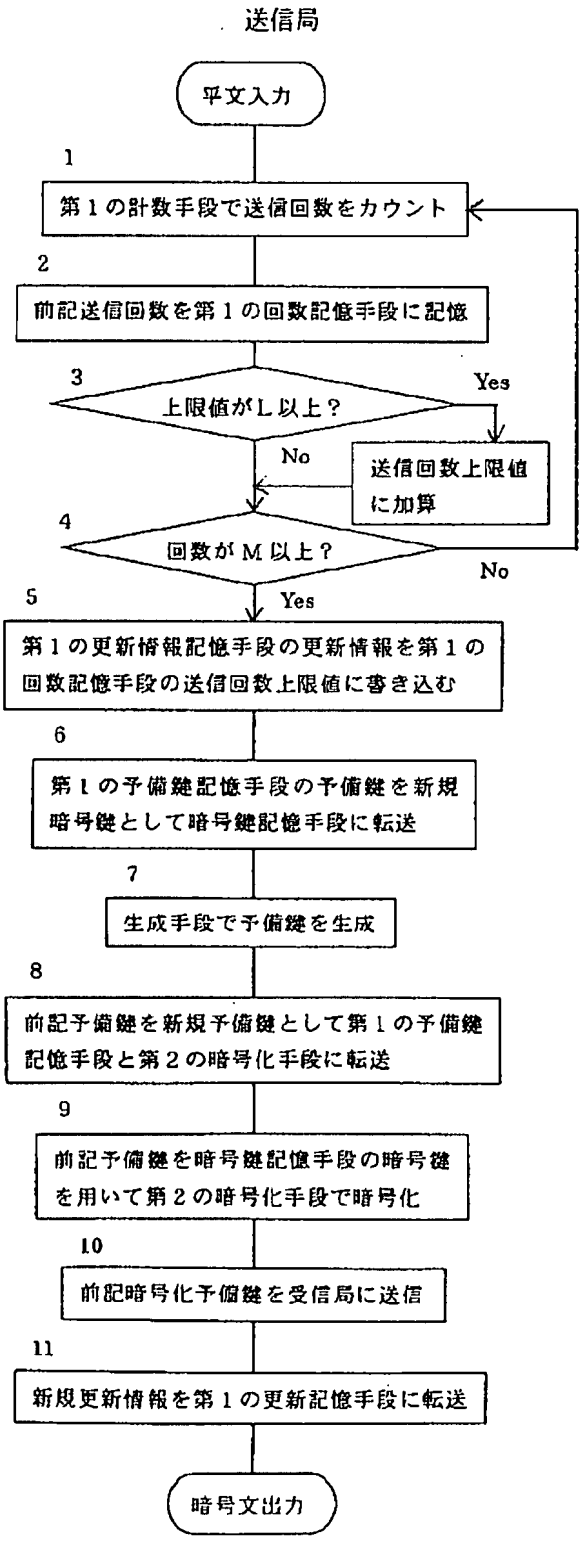
[Drawing 2]



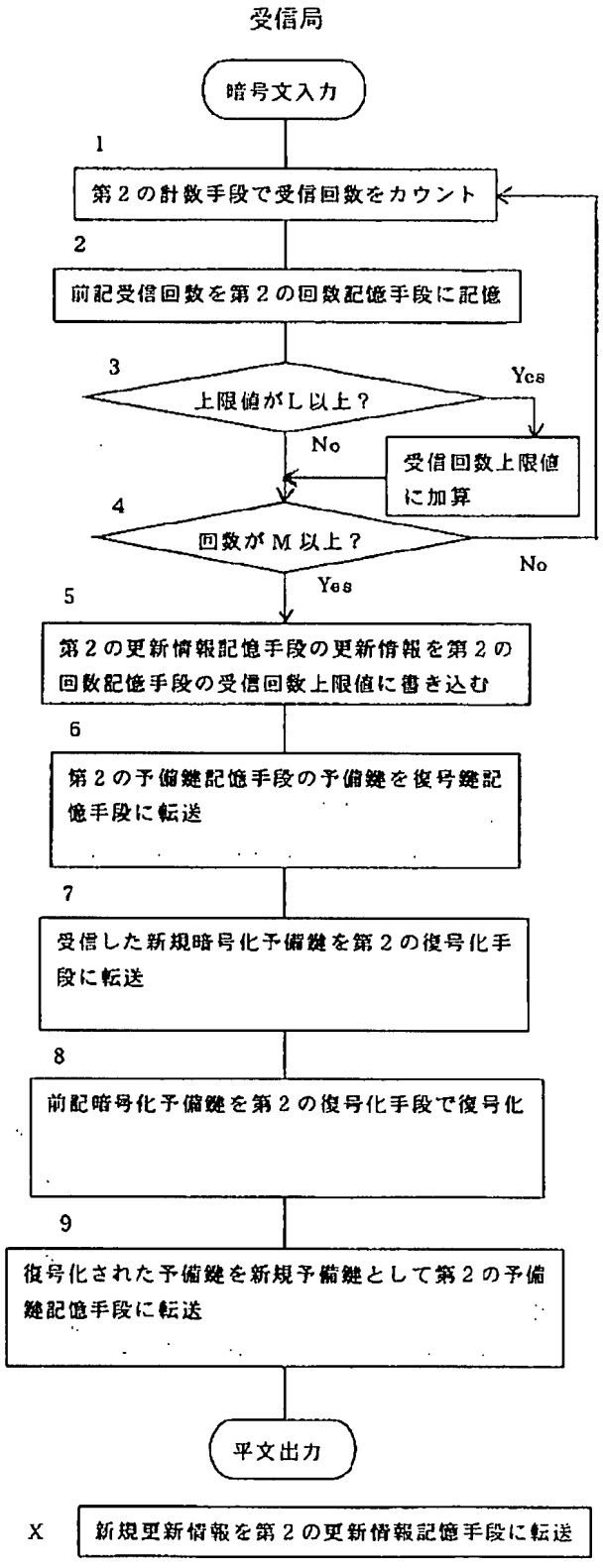
[Drawing 6]



[Drawing 3]

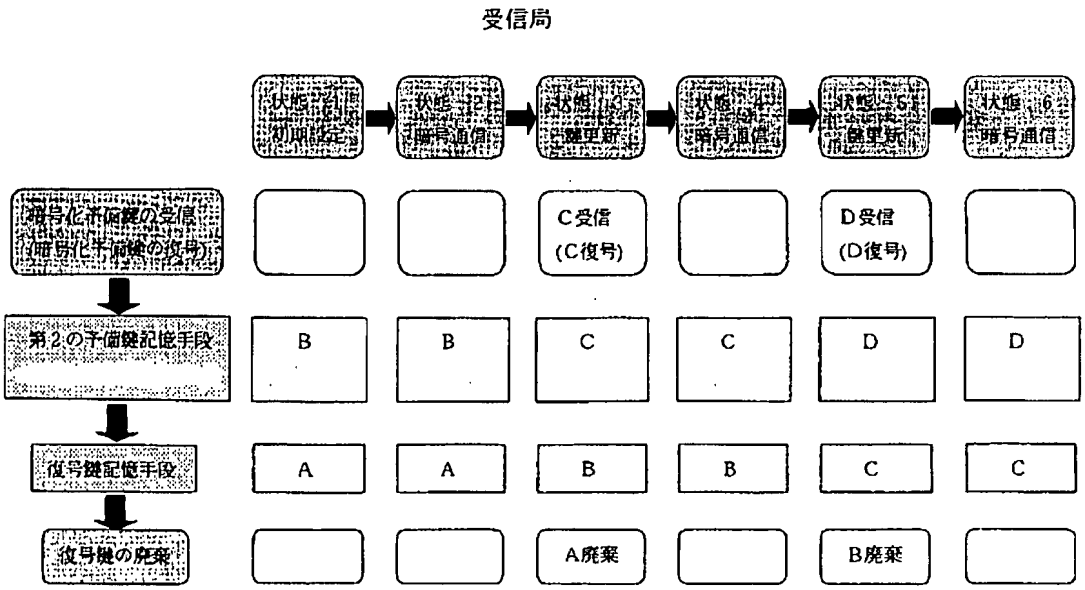

送信局
平文入力
1
第１の計数手段で送信回数をカウント
2
前記送信回数を第１の回数記憶手段に記憶
3
上限値がＬ以上？
Yes
No
送信回数上限値に加算
4
回数がＭ以上？
No
Yes
5
第１の更新情報記憶手段の更新情報を第１の回数記憶手段の送信回数上限値に書き込む
6
第１の予備鍵記憶手段の予備鍵を新規暗号鍵として暗号鍵記憶手段に転送
7
生成手段で予備鍵を生成
8
前記予備鍵を新規予備鍵として第１の予備鍵記憶手段と第２の暗号化手段に転送
9
前記予備鍵を暗号鍵記憶手段の暗号鍵を用いて第２の暗号化手段で暗号化
10
前記暗号化予備鍵を受信局に送信
11
新規更新情報を第１の更新記憶手段に転送
暗号文出力

[Drawing 4]

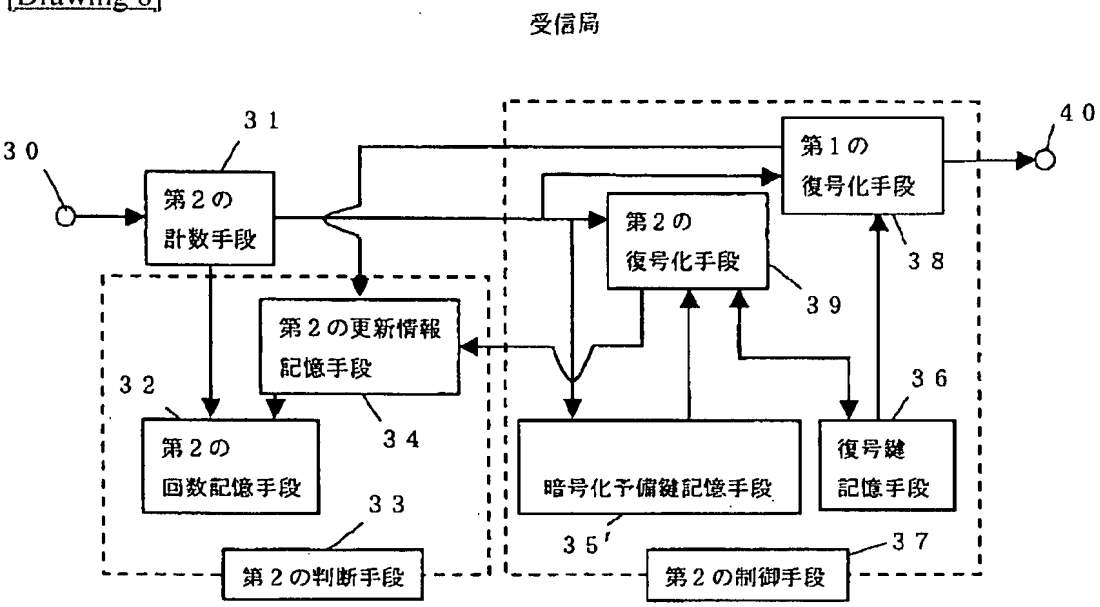


※２ Ｘは更新情報の種類によりタイミングが異なる。

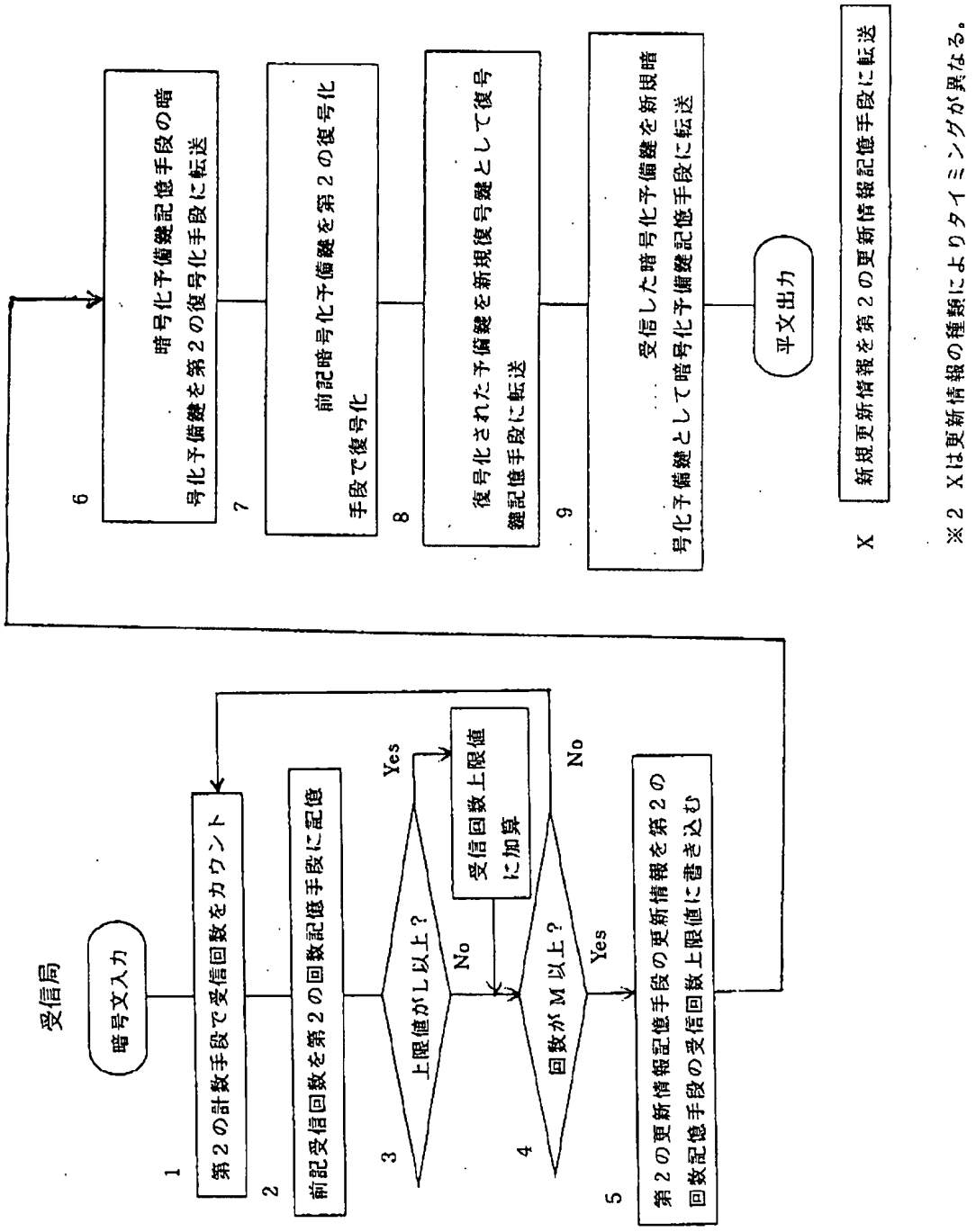
[Drawing 7]



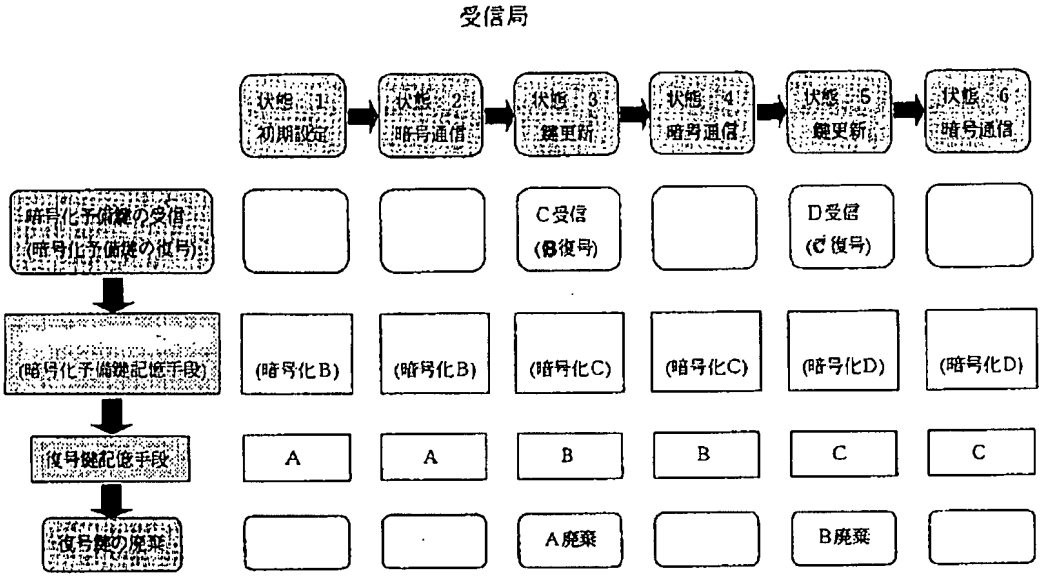
[Drawing 8]



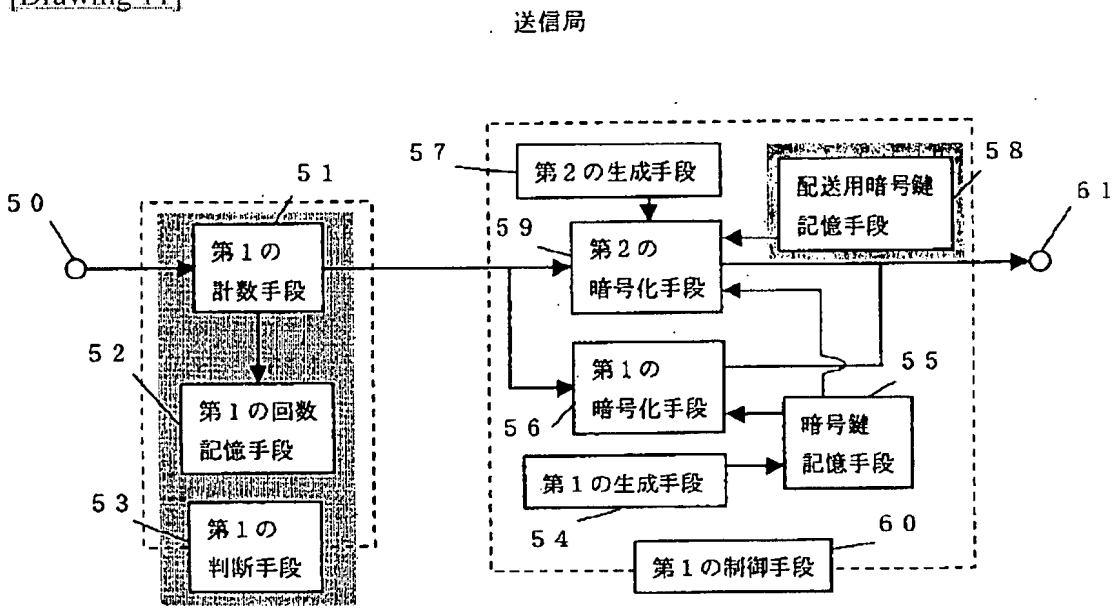
[Drawing 9]


受信局
暗号文入力
1
第２の計数手段で受信回数をカウント
2
前記受信回数を第２の回数記憶手段に記憶
3
上限値がＬ以上？
Yes
No
受信回数上限値に加算
4
回数がＭ以上？
No
Yes
5
第２の更新情報記憶手段の更新情報を第２の回数記憶手段の受信回数上限値に書き込む
6
暗号化予備鍵記憶手段の暗号化予備鍵を第２の復号化手段に転送
7
前記暗号化予備鍵を第２の復号化手段で復号化
8
復号化された予備鍵を新規復号鍵記憶手段に転送
9
受信した暗号化予備鍵を新規暗号化予備鍵として暗号化予備鍵記憶手段に転送
平文出力
X
新規更新情報を第２の更新情報記憶手段に転送
※２　Ｘは更新情報の種類によりタイミングが異なる。

[Drawing 10]

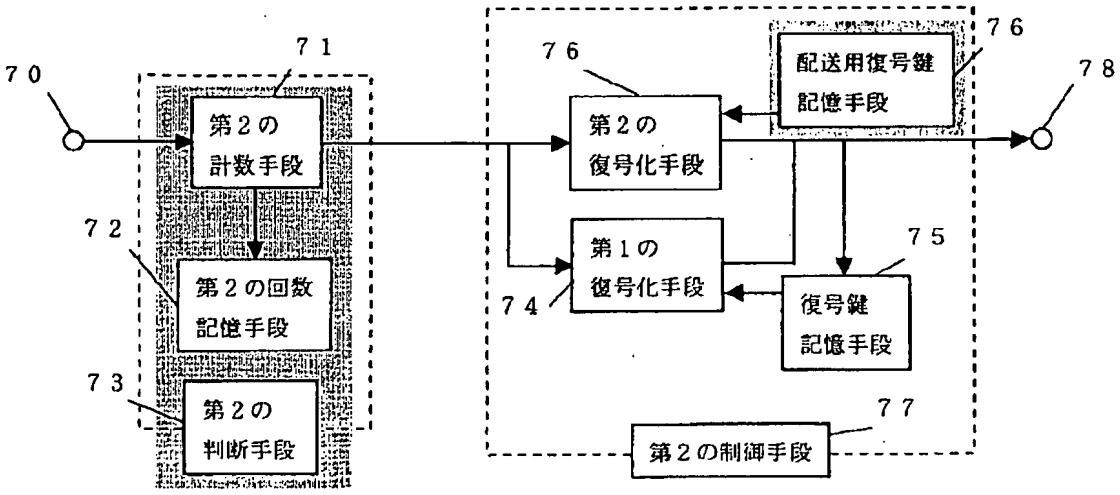


[Drawing 11]



[Drawing 12]

受信局



[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the renewal equipment of a key in the cryptocommunication equipment which used the community (secret) key block cipher for cryptocommunication and cryptographic key delivery especially about the cryptocommunication equipment which consists of a sending station and a receiving station.
[0002]
[Description of the Prior Art] The cryptocommunication equipment which used the conventional community (secret) key block cipher for cryptocommunication and cryptographic key delivery As a key delivery method for renewal of a key, encipher and deliver the new key for updating with the key which was being used before renewal of a key. (for example, JP,60-10834,A) and the key for delivery prepared independently -- enciphering -- delivering (for example, JP,62-104238,A) -- it enciphers and delivers with the key used in the past -- ** (for example, JP,1-225251,A) -- the means to say was used.
[0003] Moreover, as timing which performs renewal of a key, when there was an updating demand from whenever, sending station, or receiving station of cryptocommunication, or when use of a key reached fixed time amount (for example, JP,62-181643,A), renewal of a key was performed.
[0004] Drawing 11 and drawing 12 show the example which combined said some of advanced technology as conventional cryptocommunication equipment, drawing 11 shows the example of a sending station and drawing 12 shows the example of a receiving station. Each means of the range bundled with the dotted line is controlled by the decision means or the control means.
[0005] With conventional cryptocommunication equipment, the method which performs renewal of a key when an updating demand is at every (A) cryptocommunication as timing which performs renewal of a key from the method which performs renewal of a key, and the (B) sending station or a receiving station, when use of the (C) key reached fixed time amount, there was a method which performs renewal of a key. In drawing 11 and drawing 12 , two methods of (A) and (B) correspond, when 51, 52, 53, 71, 72, and 73 do not exist, and in drawing 11 and drawing 12 , the method of (C) corresponds, when 51, 52, 53, 71, 72, and 73 exist.
[0006] In the case of conventional (A) method data encryption equipment, a means to determine the timing of renewal of a key is not required.
[0007] (B) Since a means to determine the timing of renewal of a key does not exist in the case of method data encryption equipment, the user of a sending station or a receiving station needs to determine timing using the means of arbitration. A counter etc. can be considered, if it updates by communication link time amount and will update by the timer and the count of transmission and reception as a means of arbitration.
[0008] (C) the case of method data encryption equipment -- the conventional sending station -- the 1st counting -- the count of transmission by which counting was carried out with the means 51 is memorized by the 1st count storage means 52, the count upper limit of transmission the 1st decision means 53 was remembered to be by said count of transmission and the 1st count storage means 52 is

compared, and if equal, updating initiation will be notified to the 1st control means 60. moreover -- the conventional receiving station -- the 2nd counting -- the count of reception by which counting was carried out with the means 71 is memorized by the 2nd count storage means 72, the count upper limit of reception the 2nd decision means 73 was remembered to be by said count of reception and the 2nd count storage means 72 is compared, and if equal, updating initiation will be notified to the 2nd control means 77.

[0009] A means encipher and deliver with the key which enciphered and delivered the new key for updating as a key delivery method for renewal of a key with conventional cryptocommunication equipment with the key for delivery which enciphered and delivered with the key which was being used before renewal of (D) key, or was prepared according to (E), or was used in the past used. In drawing 11 and drawing 12 , (D) corresponds, when each 58 or 76 means do not exist, and in drawing 11 and drawing 12 , the (E) method corresponds, when each 58 or 76 means exist.

[0010] (D) In the case of a method, the 1st control means which received the notice of updating initiation performs the following control in the conventional sending station. The new key generated with the 2nd generation means 57 is enciphered with the 2nd encryption means 59 using the cryptographic key which was memorized by the cryptographic key storage means 55 and which has already been used for cryptocommunication, and it transmits to a receiving station. Moreover, in the conventional receiving station, the 2nd control means which received the notice of updating initiation performs the following control. The received new key which was enciphered is decrypted with the 2nd decryption means 76 using the decode key which was memorized by the decode key storage means 75 and which has already been used for cryptocommunication, and a new key is obtained.

[0011] (E) In the case of a method, the 1st control means which received the notice of updating initiation performs the following control in the conventional sending station. The new key generated with the 2nd generation means 57 is enciphered with the 2nd encryption means 59 using the cryptographic key for delivery memorized by the cryptographic key storage means for delivery, and it transmits to a receiving station. Moreover, in the conventional receiving station, the 2nd control means which received the notice of updating initiation performs the following control. The received new key which was enciphered is decrypted with the 2nd decryption means 76 using the decode key for delivery memorized by the decode key storage means 76 for delivery, and a new key is obtained.

[0012]

[Problem(s) to be Solved by the Invention] When updating the key used for cryptocommunication in the above-mentioned conventional cryptocommunication equipment, a means to encipher and deliver with the key which enciphered and delivered the new key for updating with the key which was being used before renewal of a key, or was used in the past was used. However, since the key used for delivery was a key which already carried out fixed period use, it had the problem that the safety of a key was low.

[0013] Moreover, when delivering with the key for delivery prepared independently, it had the problem that it will be necessary to manage the key used for delivery apart from the key used for cryptocommunication (generation, secrecy, and updating).

[0014] When updating at every cryptocommunication, in order for update process time amount to always join cryptocommunication time amount, it had the problem of taking time amount before cryptocommunication actually becomes possible.

[0015] Moreover, since in when use of a key reaches the time amount of arbitration the exchange for deciding on the time amount of arbitration between sending-station-receiving stations is needed in order to change timing It updated more often to the same timing, and had the problem that possibility that information which makes decode easy, such as which is the cipher which enciphered the key, or the cipher to where is enciphered with the same key, will be known by the tapping person became high.

[0016] Moreover, when it was a time of there being an updating demand from a sending station or a receiving station, in order that updating decision might be dependent on a user, it became a user with the burden and had the problem that the dependability of updating decision was low.

[0017] This invention shifts a use stage and enables it to use the same key for cryptocommunication and delivery with fixed safety by solving the above-mentioned conventional problem and always preparing

the key of the reserve updated periodically. Since the key used for delivery is always intact, safety sets it as the 1st purpose to offer the outstanding cryptocommunication equipment which can save the time and effort which manages the key for delivery highly (generation and updating).
[0018] Moreover, it sets it as the 2nd purpose to offer the outstanding cryptocommunication equipment which can save the time and effort to manage (secrecy) by enciphering the delivery key of a receiving station.
[0019] Moreover, since there is no need of communicating between sending-station-receiving stations whenever it changes the timing of updating by determining the timing of updating depending on a reserve key or a plaintext and the timing of updating becomes random, the information which makes the above-mentioned decode easy sets it as the 3rd purpose to offer the outstanding cryptocommunication equipment it is hard coming to specify as a tapping person.
[0020]
[Means for Solving the Problem] In this invention, in order to solve the above-mentioned technical problem, it sets to the sending station of cryptocommunication equipment. Make a reserve key into a new cryptographic key, and the reserve key generated by the generation means is used as a new reserve key. It considered as the configuration which enciphers a reserve key by the cryptographic key, transmits, enciphers transmit data by the cryptographic key after that, and is transmitted, and the reserve key was used as the new decode key in the receiving station, the reception encryption key was decrypted, and it considered as the reserve key, and considered as the configuration which decrypts reception encryption data after that. Thus, by having constituted, since a spare key is prepared and a new key is always delivered with an intact key, safety becomes high, and even if it uses the same key for cryptocommunication and key delivery, the time and effort which can update insurance and the key used for cryptocommunication simple, and manages the key for delivery (generation and updating) can be saved.
[0021] Moreover, in the receiving station of cryptocommunication equipment, the reception encryption key was memorized as an encryption reserve key, and it considered as the configuration which decrypts an encryption reserve key and is used as a new decode key in the case of renewal of a key. Thus, by having constituted, the time and effort which manages a reserve key in a receiving station (secrecy) can be saved.
[0022] Moreover, the decision means of the sending station of cryptocommunication equipment investigates the count of transmission, and the count upper limit of transmission. If the count upper limit of transmission becomes below constant value, constant value will be added to the count upper limit of transmission. If the count of transmission and the count upper limit of transmission are equal, update information will be written in the count upper limit of transmission, updating initiation is notified, and it considers as the configuration which performs the transfer to the update information storage means of new update information after that. With the decision means of a receiving station If the count of reception and the count upper limit of reception are investigated and the count upper limit of reception becomes below constant value, constant value will be added to the count upper limit of reception. If the count of reception and the count upper limit of reception were equal, update information was written in the count upper limit of reception, updating initiation was notified, and it considered as the configuration which performs the transfer to the update information storage means of new update information after that. Thus, by having constituted, the timing of updating is determined depending on a reserve key or a plaintext, and the need of communicating between sending-station-receiving stations whenever it changes the timing of updating is abolished, and the timing of updating becomes random, and a tapping person stops easily being able to specify the information which makes decode easy.
[0023]
[Embodiment of the Invention] Invention of this invention according to claim 1 is cryptocommunication equipment which consists of a sending station and a receiving station. Said sending station A cryptographic key storage means to memorize a cryptographic key, and the 1st reserve key storage means which memorizes the 1st reserve key, The 1st encryption means which enciphers data using said cryptographic key, and the 2nd encryption means which enciphers said 1st reserve key using said

cryptographic key, It transmits to said cryptographic key storage means by making into a new cryptographic key a generation means to generate said 1st reserve key, and said 1st reserve key. It transmits to said 1st reserve key storage means as 1st reserve key. new in the reserve key generated by said generation means -- It has the 1st control means which controls outputting the result of said 2nd encryption means and outputting the result of the encryption means of the account 1st of back to front. Said receiving station A decode key storage means to memorize a decode key, and the 2nd reserve key storage means which memorizes the 2nd reserve key, The 1st decryption means which decrypts encryption data using said decode key, The 2nd decryption means which decrypts the result of said 2nd encryption means using said decode key, It transmits to said decode key storage means by using said 2nd reserve key as a new decode key. It transmits to the 2nd reserve key storage means as 2nd reserve key. new in the result of said 2nd decryption means -- It is cryptocommunication equipment equipped with the 2nd control means which controls outputting the result of the decryption means of the account 1st of back to front, and the key of the reserve updated periodically is always prepared, a use stage is shifted, and it has an operation of enabling it to use the same key for cryptocommunication and delivery with fixed safety.

[0024] In cryptocommunication equipment according to claim 1, said 1st encryption means in a sending station decrypts encryption data using said cryptographic key, said 1st decryption means in a receiving station enciphers data using said decode key, and invention of this invention according to claim 2 has an operation of making it possible to send encryption data to a sending station from a receiving station.

[0025] Invention of this invention according to claim 3 is set to cryptocommunication equipment according to claim 1. A decode key storage means by which said receiving station memorizes a decode key, and an encryption reserve key storage means to memorize the result of said 2nd encryption means, The 1st decryption means which decrypts the result of said 1st encryption means using said decode key, The 2nd decryption means which decrypts the result of said 2nd encryption means using said decode key, It is a thing equipped with the 2nd control means which controls transmitting the result of said 2nd encryption means to an encryption reserve key storage means, and transmitting to said decode key storage means by using the result of said 2nd decryption means as a new decode key. By enciphering the delivery key of a receiving station, it has an operation of saving the time and effort to manage (secrecy).

[0026] Invention of this invention according to claim 4 is set to cryptocommunication equipment according to claim 1. Said sending station the 1st counting which carries out counting of the count of transmission -- with a means and the 1st count storage means which memorizes said count of transmission, and said count upper limit of transmission An update information storage means, and the 1st said count of transmission and said count upper limit of transmission which memorizes update information are investigated. If said count upper limit of transmission becomes below constant value, constant value will be added to said count upper limit of transmission. If said count of transmission and said count upper limit of transmission are equal, said update information will be written in said count upper limit of transmission. Updating initiation is notified and it has the 1st decision means which performs the transfer to said update information storage means of new update information after that. Said receiving station the 2nd counting which carries out counting of the count of reception -- with a means and the 2nd count storage means which memorizes said count of reception, and said count upper limit of reception If said count of reception and said count upper limit of reception are investigated and said count upper limit of reception becomes below constant value, constant value will be added to said count upper limit of reception. If said count of reception and said count upper limit of reception are equal, said update information will be written in said count upper limit of reception. Updating initiation is notified, it has the 2nd decision means which performs the transfer to said update information storage means of new update information after that, the timing of updating is determined according to a reserve key or a plaintext, and it has the operation of making hard to specify information which makes decode easy.

[0027] Hereafter, the gestalt of operation of this invention is explained to a detail using drawing 10 from drawing 1 .

[0028] (Gestalt of the 1st operation) The gestalt of operation of the 1st of this invention In a sending

station, transmit the result of having enciphered the reserve key by the cryptographic key, transmit the result of having enciphered data by the cryptographic key after that, and it sets to a receiving station. It is cryptocommunication equipment which transmits to a decode key storage means by using the reserve key in a reserve key storage means as a new decode key, outputs the result of having decoded the reception encryption reserve key with the decode key to a reserve key storage means, and outputs the result of having decoded reception encryption data with the decode key after that.
[0029] Drawing 1 is the block diagram of the sending station of the cryptocommunication equipment of the gestalt of operation of the 1st of this invention. In drawing 1 , each means of the range bundled with the dotted line is controlled by the decision means or the control means.
[0030] In drawing 1 , an input terminal 10 performs a plaintext entry of data at the time of transmission, and consists of connectors.
[0031] the 1st counting -- a means 11 carries out counting of the count of transmission of data, and transmission of data is performed in fact -- ** -- the microprocessor which was alike, adds 1 to the count of transmission memorized by the 1st count storage means 12, and built in ROM and RAM, for example, CPU, DSP, etc. -- counting -- counting which programmed the algorithm -- it is what was considered as Dedication LSI, and it is constituted.
[0032] the 1st count storage means 12 -- the 1st counting -- it is the memory which memorizes the count upper limit of transmission which determines the timing of renewal of a key as the current count of transmission by which counting was carried out with the means 11, for example, consists of RAM etc.
[0033] The 1st decision means 13 is whether it reached more than the count with the fixed count of transmission of the data memorized by the 1st count storage means 12, and a thing which updates the count upper limit of transmission while judging. In fact The current count of transmission and the current count upper limit of transmission which are memorized by the 1st count storage means 12 are compared. Actuation of transmitting the update information memorized by the 1st update information storage means 14 to the 1st count storage means 12 if equal, notifying updating initiation to the 1st control means 18, and transmitting new update information to the 1st update information storage means 14, If the count upper limit of transmission of the 1st count storage means 12 becomes below the number set up beforehand, actuation of adding constant value is performed, and it is what was made only into for [LSI] the decision which programmed the decision algorithm to the microprocessor which built in ROM and RAM, for example, CPU, DSP, etc., and is constituted. The renewal of the count upper limit of transmission performs update information transmitted from the 1st update information storage means 14 by overwriting the count upper limit of transmission of the 1st count storage means 12. However, the count upper limit of transmission is performed only for updating by 0 times, and the problem that it does not shift to a cryptocommunication condition arises. Moreover, if updating is frequently performed by the count of a single figure, the processing time will increase and trouble will be caused to employment. In order to avoid this problem, the count upper limit of transmission performs actuation of adding constant value, at the time of 0 times or the count of a single figure. Moreover, actual communication link frequency should determine the scope and aggregate value of the count upper limit of transmission. It is possible to use a reserve key and a plaintext as update information. A fixed number of bits are transmitted to the 1st update information storage means 14 from the specific location (for example, a head or the rear) of the reserve key which was generated with the 1st generation means 15 in the case of the reserve key. A fixed number of bits are transmitted to an update information storage means from the specific location (for example, a head or the rear) of the plaintext which enciphers first in the case of a plaintext, and transmits to it after renewal of a key. Moreover, if the period of renewal of a key can be determined as the fixed range, for example, it is made 8 bits by into what bit update information to transmit is made, it can be decided that they will be 0 - 255 times of range.
[0034] The 1st update information storage means 14 is memory which memorizes update information, for example, consists of RAM etc.
[0035] The generation means 15 generates a reserve key (pseudo-random number), is what was made only into for [LSI] the generation which programmed the generation algorithm to the microprocessor which built in ROM and RAM, for example, CPU, DSP, etc., and is constituted. As a random-number

generation algorithm, it is common to use LFSR (Liner Feedback Shift Registers). However, if combination is possible, cryptographic algorithm and a hash algorithm may be used. Moreover, the initial value called seed is required for pseudo-random number generation, for example, system clocks, such as CPU-DSP, can be used as seed.

[0036] The 1st reserve key storage means 16 is memory which memorizes the reserve key generated with the 1st generation means 15, for example, consists of RAM etc.

[0037] The cryptographic key storage means 17 is memory which memorizes the cryptographic key used for encryption with the 1st encryption means 19 and the 2nd encryption means 20, for example, consists of RAM etc.

[0038] When the notice of updating initiation is received, the 1st control means 18 is controlled to perform the following actuation in order, is what was made only into for [LSI] the control which programmed the control algorithm to the microprocessor which built in ROM and RAM, for example, CPU-DSP etc., and is constituted. The reserve key beforehand memorized by introduction and the 1st reserve key storage means 16 is transmitted to the cryptographic key storage means 17. Next, generation of a reserve key is directed for the generation means 15, it transmits to the 1st reserve key storage means 16 and the 2nd encryption means 20 by using this generated reserve key as a new reserve key next, then, encryption of this reserve key is directed for the 2nd encryption means 20, and, finally this encryption cryptographic key is transmitted to a receiving station.

[0039] The 1st encryption means 19 enciphers data using the cryptographic key memorized by the cryptographic key storage means 17, is what was made only into for [LSI] the codes which programmed cryptographic algorithm to the microprocessor which built in ROM and RAM, for example, CPU-DSP etc., and is constituted. However, if it is troublesome to program cryptographic algorithm to the microprocessor which built in ROM and RAM, for example, CPU, DSP, etc., what is developed as LSI only for codes and marketed from the start can also be used. Moreover, although the community (secret) key block cipher is used as a code and DES-FEAL-IDEA etc. is mentioned as the class in this invention, even if it uses which code, it is thought that this invention is effective.

[0040] The 2nd encryption means 20 enciphers a key using the cryptographic key memorized by the cryptographic key storage means 17, and is the same as the 1st encryption means.

[0041] An output terminal 21 outputs encryption data at the time of transmission, outputs plaintext data at the time of reception, and consists of connectors etc.

[0042] Drawing 2 is the block diagram of the receiving station of the cryptocommunication equipment of the gestalt of operation of the 1st of this invention. In drawing 2 , each means of the range bundled with the dotted line is controlled by the decision means or the control means. In drawing 2 , an input terminal 30 performs an encryption entry of data at the time of reception, and consists of connectors.

[0043] the 2nd counting -- a means 31 carries out counting of the count of reception of data, and reception of data is performed in fact -- ** -- the microprocessor which was alike, adds 1 to the count of reception memorized by the 2nd count storage means 32, and built in ROM and RAM, for example, CPU, DSP, etc. -- counting -- counting which programmed the algorithm -- it is what was considered as Dedication LSI, and is constituted.

[0044] the 2nd count storage means 32 -- the 2nd counting -- it is the memory which memorizes the count upper limit of reception which determines tie MISHIGU of the current count of reception by which counting was carried out with the means 31, and renewal of a key, for example, consists of RAM etc.

[0045] The 2nd decision means 33 is whether it reached more than the count with the fixed count of reception of the data memorized by the 2nd count storage means 32, and a thing which updates the count upper limit of reception while judging. In fact The count upper limit of reception set up beforehand is compared with the current count of reception memorized by the count storage means 32. Actuation of transmitting the update information memorized by the 2nd update information storage means 34 to the 2nd count storage means 32 if equal, notifying updating initiation to the 2nd control means 37, and transmitting new update information to the update information storage means 34, If the count upper limit of reception of the 2nd count storage means 32 becomes below the number set up beforehand,

actuation of adding constant value is performed, and it is what was made only into for [LSI] the decision which programmed the decision algorithm to the microprocessor which built in ROM and RAM, for example, CPU-DSP etc., and is constituted. Renewal of the count upper limit of reception is performed by overwriting the update information transmitted from the 2nd update information storage means 34 at the count upper limit of reception of the 2nd count storage means 32. However, the count upper limit of reception is performed only for updating by 0 times, and the problem that it does not shift to a cryptocommunication condition arises. Moreover, if updating is frequently performed by the count of a single figure, the processing time will increase and trouble will be caused to employment. In order to avoid this problem, the count upper limit of reception performs actuation of adding constant value, at the time of 0 times or the count of a single figure. Moreover, actual communication link frequency should determine the scope and aggregate value of the count upper limit of reception. It is possible to use a reserve key and a plaintext as update information. In order to use a reserve key, a fixed number of bits are transmitted to the 2nd update information storage means from the specific location (for example, a head or the rear) of the reserve key decrypted with the 2nd decryption means 38. A fixed number of bits are transmitted to the 2nd update information storage means 34 from the specific location (for example, a head or the rear) of the plaintext which received first in the case of the plaintext, and was decrypted with the 1st decryption means 39 after renewal of a key in it. Moreover, the period of renewal of a key can be determined as the fixed range by into what bit update information to transmit is made, for example, if it is made 8 bits, it can be decided that they will be 0 - 255 times of range.

[0046] The 2nd update information storage means 34 is memory which memorizes update information, for example, consists of RAM etc.

[0047] The 2nd reserve key storage means 35 is memory which memorizes a reserve key, for example, consists of RAM etc.

[0048] The decode key storage means 36 is memory which memorizes a decode key, for example, consists of RAM etc.

[0049] When the notice of updating initiation is received, the 2nd control means 37 is controlled to perform the following actuation in order, is what was made only into for [LSI] the control which programmed the control algorithm to the microprocessor which built in ROM and RAM, for example, CPU-DSP etc., and is constituted. It transmits to the decode key storage means 36 by using as a new decode key the reserve key beforehand memorized by introduction and the 2nd reserve key storage means 35. Next, the received encryption reserve key is transmitted to the 2nd decryption means 38, and next, a decryption of said encryption reserve key is directed for the 2nd decryption means 38, and it transmits to the 2nd reserve key storage **** by using as a new reserve key the reserve key decrypted at the end.

[0050] The 1st decryption means 38 decrypts data using the decode key memorized by the decode key storage means 36, is what was made only into for [LSI] the codes which programmed cryptographic algorithm to the microprocessor which built in ROM and RAM, for example, CPU-DSP etc., and is constituted. However, if it is troublesome to program cryptographic algorithm to the microprocessor which built in ROM and RAM, for example, CPU-DSP etc., what was developed as LSI only for codes from the start like the sending station can also be used. Moreover, although the community (secret) key block cipher is used as a code and DES-FEAL-IDEA etc. is mentioned as the class in this invention, even if it uses which code, it is thought that this invention is effective.

[0051] The 2nd decryption means 39 decrypts a key using the decode key memorized by the decode key storage means 36, and is the same as the 1st decryption means.

[0052] An output terminal 40 outputs data at the time of reception, and consists of connectors.

[0053] About the cryptocommunication equipment constituted as mentioned above, the actuation is explained using drawing 3 and drawing 4 . Drawing 3 shows actuation of a sending station and drawing 4 shows actuation of a terminal here. Drawing 3 is explained.

[0054] Introduction and the correspondence (plaintext) which transmits to a receiving station as an input are considered. Even steps 1-4 are the processes which judge shift of renewal pro SESUHE of a key.

[0055] step 1-2 -- the 1st counting -- a means 11 checks that the transmit data has been sent as an input,

and adds 1 to the count of transmission memorized by the 1st count storage means 12.
[0056] With [the count upper limit of transmission memorized by the 1st count storage means 12] L [below], at step 3, constant value is added to a upper limit.
[0057] At step 4, the upper limit M of the count of transmission memorized by the 1st count storage means 12 and the count of transmission is compared, if equal, updating initiation will be notified to the 1st control means 13, otherwise, it returns to step 1. All actuation after step 5 is renewal processes of a key performed in order by the 1st control means 13.
[0058] At step 5, the update information memorized by the 1st update information storage means 14 is overwritten at the count upper limit of transmission of the 1st count storage means 12.
[0059] At step 6, it transmits to the cryptographic key storage means 17 by making into a new cryptographic key the reserve key memorized by the 1st reserve key storage means 16.
[0060] At step 7, the generation means 15 generates a reserve key (pseudo-random number).
[0061] At step 8, it transmits to the 1st reserve key storage means 16 and the 2nd encryption means 20 by using as a new reserve key the reserve key generated at step 7.
[0062] At step 9, the reserve key transmitted to the 2nd encryption means 20 at step 8 is enciphered by the cryptographic key memorized by the cryptographic key storage means 17.
[0063] At the . step 11 which transmits the encryption reserve key generated at step 9 to a receiving station at step 10, new update information is transmitted to the 1st update information storage means 14. Correspondence (input plaintext) is enciphered and outputted after step 11 termination using the cryptographic key updated as an output.
[0064] Drawing 4 is explained. Even steps 1-4 are the processes which judge shift of renewal pro SESUHE of a key.
[0065] step 1-2 -- the 2nd counting -- a means 31 checks that received data have been sent as an input, and adds 1 to the count of reception memorized by the 2nd count storage means 32.
[0066] With [the count upper limit of reception the 2nd decision means 33 is remembered to be by the 2nd count storage means 32] L [below], at step 3, constant value is added to a upper limit.
[0067] At step 4, the upper limit M of the count of reception the count upper limit of reception memorized by the 2nd count storage means 32 is remembered to be by the 2nd count storage means 32, and the count of reception is compared, if equal, updating initiation will be notified to the 2nd control means 33, otherwise, it returns to step 1. All actuation after step 5 is renewal processes of a key performed in order by the 2nd control means 37.
[0068] At step 5, the update information memorized by the 2nd update information storage means 34 is written in the count upper limit of reception of the 2nd count storage means 32.
[0069] At step 6, the reserve key memorized by the 2nd reserve key storage means 35 is transmitted to the decode key storage means 36.
[0070] At step 7, the received encryption reserve key is transmitted to the 2nd decryption means 39.
[0071] At step 8, the encryption reserve key transmitted at step 7 is decrypted using the decode key memorized by the decode key storage means 36 with the 2nd decryption means 39.
[0072] At step 9, it transmits to the 2nd reserve key storage means 35 by using as a new decode key the reserve key decrypted at step 8.
[0073] As for step X, the timing by which new update information is performed with a plaintext or a reserve key differs. If it is a reserve key, it will perform after the step 8 termination by which a reserve key is decrypted. It performs, after the plaintext which decrypts the cipher received first and is obtained after the renewal termination of a key comes to hand in the case of a plaintext.
[0074] Drawing 5 shows the configuration of the whole cryptocommunication equipment which connected the sending station and the receiving station. Connection of the input/output terminal 21 of a sending station and the input/output terminal 30 of a receiving station assumes the cable, and is constituted from this invention by the cable, for example, a coaxial cable. Moreover, it is thought that the renewal equipment of a key of this invention is usable also to a radio communications system. In drawing 5 , although the receiving station shows only one set for simplification of explanation, two or more receiving stations are assumed in fact. A sending station is a base station and this is because it

thinks also case [whose receiving station is / like a terminal station]. When a receiving station is plurality, the receiving station side is also the same as that of old explanation. However, since only the number of a receiving station needs to perform renewal of a key, a sending station must divide and memorize a key, the count of transmission, and the count upper limit of transmission for every receiving station. That is, for the 1st count storage means of a sending station, the 1st reserve key storage means, and the 1st cryptographic key storage means, the count of transmission, the count upper limit of transmission, reserve key, and cryptographic key for every receiving station are memorized, respectively.

[0075] as the important matter on mounting -- the 1st counting of a sending station -- since effectiveness is bad when a microprocessor is used and a means 11, the 1st decision means 13, the 1st control means 18, the generation means 15, the 1st encryption means 19, and the 2nd encryption means 20 are constituted separately, if there is no problem in the engine performance, it is desirable to make it serve a double purpose by one microprocessor. moreover -- a receiving station -- the same -- the 2nd counting -- it is desirable to make a means 31, the 2nd decision means 33, the 2nd control means 37, the 1st decryption means 38, and the 2nd decryption means 39 serve a double purpose by one microprocessor.

[0076] Drawing 6 and drawing 7 are what showed arrangement of the key in each communication link condition, a longitudinal direction expresses a communication link condition and a lengthwise direction expresses the condition of a key.

[0077] As for the case of the sending station shown in drawing 6 , **** of a key changes as follows.

[0078] Condition: 1 is the preparation phase before communicating and sets Key A and Key B first. Moreover, the initial value of the upper limit of the count of transmission which updates a key, and the count of reception is determined as coincidence between the sending station and the receiving station at this time.

[0079] Condition: 2 is in the first cryptocommunication condition, and perform cryptocommunication by the cryptographic key A of a cryptographic key storage means, and don't use the reserve key B of the 1st reserve key storage means 16. The count of transmission is a time of reaching constant value, and shifts to condition:3.

[0080] Condition: 3 is the first letter bear of renewal of a key, by making the reserve key B of the 1st reserve key storage means 16 into a new cryptographic key, is transmitted to the cryptographic key storage means 17, and is taken as a cryptographic key B. It means that the cryptographic key A was discarded by this. Next, Key C is generated and it transmits to the 1st reserve key storage means 16 as a new reserve key. Finally the reserve key C is enciphered by the cryptographic key B, and it transmits, and shifts to condition:4.

[0081] Condition: 4 is in a cryptocommunication condition, and perform cryptocommunication by the cryptographic key B of the cryptographic key storage means 17, and don't use the reserve key C of the 1st reserve key storage means 16. It is a time of the count upper limit of transmission reaching constant value, and shifts to condition:5.

[0082] Condition: 5 is a letter bear of renewal of a key, by making the reserve key C of the 1st reserve key storage means 16 into a new cryptographic key, is transmitted to the cryptographic key storage means 17, and is taken as a cryptographic key C. It means that the cryptographic key B was discarded by this. Next, Key D is generated and it transmits to the 1st reserve key storage means 16 as a new reserve key. Finally the reserve key D is enciphered by the cryptographic key C, and it transmits, and shifts to condition:6.

[0083] Condition: 6 is a cryptocommunication-like bear, and perform cryptocommunication by the cryptographic key C of the cryptographic key storage means 17, and don't use the reserve key D of the 1st reserve key storage means 16. Hereafter, the letter bear of key delivery and a cryptocommunication condition are repeated by turns.

[0084] As for the case of the receiving station shown in drawing 7 , the condition of a key changes as follows.

[0085] Condition: 1 is the preparation phase before communicating and sets Key A and Key B first. Moreover, the initial value of the upper limit of the count of transmission which updates a key, and the

count of reception is determined as coincidence between the sending station and the receiving station at this time.

[0086] Condition: 2 is in the first cryptocommunication condition, the decode key A of the decode key storage means 36 performs cryptocommunication, and don't use the reserve key B of the 2nd reserve key storage means 35, but when the count of reception reaches constant value, it carries out condition:3 HE shift.

[0087] Condition: 3 is in the first renewal condition of a key, by using the reserve key B of the 2nd reserve key storage means 35 as a new decode key, is transmitted to the decode key storage means 36, and is taken as the decode key B. Therefore, it means that the decode key A was discarded. Next, Encryption C is received, and it decrypts with the decode key B, and transmits to the 2nd reserve key storage 35 as a new reserve key. After the renewal termination of a key, a condition: Shift to 4.

[0088] Condition: 4 is in a cryptocommunication condition, and the decode key B of the decode key storage means 36 performs cryptocommunication, and don't use the reserve key C of the 2nd reserve key storage means 35. When the count of reception reaches constant value, it shifts to condition:5.

[0089] Condition: 5 is in the renewal condition of a key, by using the reserve key C of the 2nd reserve key storage means 35 as a new decode key, is transmitted to the decode key storage means 36, and is taken as the decode key C. Therefore, it means that the decode key B was discarded. Next, Encryption D is received, and it decrypts with the decode key C, and transmits to the 2nd reserve key storage 35 as a new reserve key. After the renewal termination of a key, a condition: Shift to 6.

[0090] Condition: 6 is in a cryptocommunication condition, and the decode key C of the decode key storage means 36 performs cryptocommunication, and don't use the reserve key D of the 2nd reserve key storage means 35. Hereafter, the letter bear of key delivery and a cryptocommunication condition are repeated by turns.

[0091] When the safety by renewal of conventional cryptocommunication equipment and the key of this invention sees as a whole at the last, it explains how it thinks. This invention is sharing the key for codes, and the key for delivery with one key by shifting a time. Since this approach uses the key intact to cryptocommunication for the key for delivery, its safety is higher than the case where the key for delivery is not prepared. However, if the cipher which enciphered the reserve key which the tapping person could decode the key for codes, and was delivered before is held, safety may become low from the case where the key for delivery is prepared independently. However, the cipher which enciphered the reserve key by making timing of renewal of a key random is made hard to specify. Therefore, if it continues using the same delivery key when preparing the key for delivery independently, possibility that the direction of the safety of this invention will become high is high.

[0092] as mentioned above, with the gestalt of operation of the 1st of this invention Transmit the result of having enciphered the reserve key for cryptocommunication equipment by the cryptographic key in the sending station, transmit the result of having enciphered data by the cryptographic key after that, and it sets to a receiving station. It transmits to a decode key storage means by using the reserve key in a reserve key storage means as a new decode key. Since it considered as the configuration which outputs the result of having decoded the reception encryption reserve key with the decode key to a reserve key storage means, and outputs the result of having decoded reception encryption data with the decode key after that and a reserve key is delivered with an intact key, the safety of key delivery becomes high.

[0093] (Gestalt of the 2nd operation) The gestalt of operation of the 2nd of this invention is cryptocommunication equipment which transmits a reception encryption reserve key to an encryption reserve key storage means, and is transmitted to a decode key storage means by using as a new decode key the result of having decoded the encryption reserve key of an encryption reserve key storage means with the decode key on the occasion of renewal of a key in a receiving station.

[0094] The place where the cryptocommunication equipment of the gestalt of the 2nd operation differs from the gestalt of the 1st operation is a point which carries out a double sign just before memorizing the reserve key by the receiving side with the encryption reserve key and using it as a decode key.

[0095] Drawing 8 is the block diagram of the receiving station of the cryptocommunication equipment of the gestalt of operation of the 2nd of this invention. drawing 8 -- setting -- an input terminal 30 and

the 2nd counting -- a means 31, the 2nd count storage means 32, the 2nd decision means 33, the 2nd update information storage means 34, the decode key storage means 36, the 1st decryption means 38, the 2nd decryption means 39, and an output terminal 40 are the same as the gestalt of the 1st operation.
[0096] The encryption reserve key storage means 35 is memory which memorizes the received encryption reserve key.
[0097] The 2nd control means 37 will be controlled to perform the following actuation in order, if the notice of updating initiation is received. The encryption reserve key of introduction and an encryption reserve key storage means 35 transmits to the 2nd decryption means 38, and next, a decryption of said encryption reserve key directs for the 2nd decryption means 38, it transmits to a decode key storage means 36, the encryption reserve key which received at the end carries out as a new encryption reserve key by using as a new decode key the reserve key decrypted next, and it transmits to an encryption reserve key storage means.
[0098] About the cryptocommunication equipment constituted as mentioned above, actuation of a receiving station is explained using the flow chart of the receiving station shown in drawing 9 . Actuation of a sending station is the same as the gestalt of the 1st operation. The process to steps 1-5 is the same as the gestalt of the 1st operation.
[0099] At step 6, the encryption reserve key memorized by encryption reserve key storage means 35' is transmitted to the 2nd decryption means 39.
[0100] At step 7, the encryption reserve key transmitted at step 6 is decoded using the decode key memorized by the decode key storage means 36 with the 2nd decryption means 39.
[0101] At step 8, it transmits to the decode key storage means 36 by using as a new decode key the reserve key decrypted at step 7.
[0102] At step 9, it transmits to encryption reserve key storage means 35' by using the received encryption reserve key as a new encryption reserve key.
[0103] As for step X, the timing by which new update information is performed with a plaintext or a reserve key differs. If it is a reserve key, it will perform after the step 8 termination by which a reserve key is decrypted. It performs, after the plaintext which decrypts the cipher received first and is obtained after the renewal termination of a key comes to hand in the case of a plaintext.
[0104] Drawing 10 is what showed arrangement of the key in each communication link condition of a receiving station, a longitudinal direction expresses a communication link condition and a lengthwise direction expresses the condition of a key. The condition of a key changes as follows.
[0105] Condition: 1 is the preparation phase before communicating and sets the encryption B which enciphered Key A and Key B with Key A first. Moreover, the initial value of the upper limit of the count of transmission which updates a key, and the count of reception is determined as coincidence between the sending station and the receiving station at this time.
[0106] Condition: 2 is in the first cryptocommunication condition, and the decode key A of the decode key storage means 36 performs cryptocommunication, and don't use the encryption B of encryption reserve key storage means 35'. It is a time of the count of reception reaching constant value, and condition:3 HE shift is carried out.
[0107] Condition: 3 is in the first renewal condition of a key, decrypts the encryption B of encryption reserve key storage means 35' with the decode key A, and transmits it to the decode key storage means 36. Therefore, it means that the decode key A was discarded. Next, Encryption C is received and it transmits to encryption reserve key storage means 35' as a new encryption reserve key. After the renewal termination of a key, a condition: Shift to 4.
[0108] Condition: 4 is in a cryptocommunication condition, and the decode key B of the decode key storage means 36 performs cryptocommunication, and don't use the encryption C of encryption reserve key storage means 35'. The count of reception is a time of reaching constant value, and shifts to condition:5.
[0109] Condition: 5 is in the renewal condition of a key, decrypts the encryption C of encryption reserve key storage means 35' with the decode key B, and transmits it to the decode key storage means 36. Therefore, it means that the decode key B was discarded. Next, Encryption D is received and it transmits

to encryption reserve key storage means 35' as a new encryption reserve key. After the renewal termination of a key, a condition: Shift to 6.
[0110] Condition: 6 is in a cryptocommunication condition, and the decode key C of the decode key storage means 36 performs cryptocommunication, and don't use the encryption D of encryption reserve key storage means 35'. Hereafter, the letter bear of key delivery and a cryptocommunication condition are repeated by turns.
[0111] as mentioned above, with the gestalt of operation of the 2nd of this invention In a receiving station, a reception encryption reserve key is transmitted for cryptocommunication equipment to an encryption reserve key storage means. Since it considered as the configuration transmitted to a decode key storage means by using as a new decode key the result of having decoded the encryption reserve key of an encryption reserve key storage means with the decode key in the case of renewal of a key, it can save, where a key is enciphered and is lost in the need of establishing separately a means to manage a delivery key (secrecy).
[0112] In addition, although the gestalt of the 1st and the 2nd operation explained the actuation which transmits in a sending station and is received in a receiving station, it can encipher using the decode key of a receiving station, and can also decrypt using the cryptographic key of a sending station.
[0113]
[Effect of the Invention] As mentioned above, since according to this invention the reserve key updated for every key delivery in cryptocommunication equipment was prepared, and the control means was considered as the configuration which controls a transfer sequence using this reserve key so that the key for delivery might always turn into an intact cryptographic key to cryptocommunication, the effectiveness that safety becomes high only in a part to deliver with an intact key is acquired.
[0114] Moreover, in this invention, since one key can be used for key delivery and cryptocommunication with fixed safety, the effectiveness that the need of managing a delivery key independently (generation and updating) is lost is acquired.
[0115] Moreover, in this invention, since it can save where a key is enciphered, the effectiveness that the need of managing a delivery key independently (secrecy) is lost is acquired.
[0116] moreover -- this invention -- transmission or the count of reception -- timing -- carrying out -- counting -- since it considered as the configuration which performs renewal of a key periodically by carrying out counting with a means and notifying that the decision means became the count of fixed, while processing becomes light, renewal of a key is performed automatically and the effectiveness of a burden stopping starting a user is acquired.
[0117] Moreover, in this invention, since tie MISHIGU is updated with a decision means depending on update information at every renewal of a key, the effectiveness that possibility that information will be known by the tapping person becomes low is acquired.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is cryptocommunication equipment which consists of a sending station and a receiving station. Said sending station A cryptographic key storage means to memorize a cryptographic key, and the 1st reserve key storage means which memorizes the 1st reserve key, The 1st encryption means which enciphers data using said cryptographic key, and the 2nd encryption means which enciphers said 1st reserve key using said cryptographic key, It transmits to said cryptographic key storage means by making into a new cryptographic key a generation means to generate said 1st reserve key, and said 1st reserve key. It transmits to said 1st reserve key storage means as 1st reserve key. new in the reserve key generated by said generation means -- It has the 1st control means which controls outputting the result of said 2nd encryption means and outputting the result of the encryption means of the account 1st of back to front. Said receiving station A decode key storage means to memorize a decode key, and the 2nd reserve key storage means which memorizes the 2nd reserve key, The 1st decryption means which decrypts encryption data using said decode key, The 2nd decryption means which decrypts the result of said 2nd encryption means using said decode key, It transmits to said decode key storage means by using said 2nd reserve key as a new decode key. new in the result of said 2nd decryption means -- the cryptocommunication equipment characterized by having the 2nd control means which controls transmitting to the 2nd reserve key storage means as 2nd reserve key, and outputting the result of the decryption means of the account 1st of back to front.
[Claim 2] Cryptocommunication equipment according to claim 1 characterized by for said 1st encryption means in a sending station decrypting encryption data using said cryptographic key, and said 1st decryption means in a receiving station enciphering data using said decode key.
[Claim 3] The cryptocommunication equipment according to claim 1 characterized by to have the 2nd control means by which said receiving station controls transmitting the result of an encryption reserve key storage means memorize the result of said 2nd encryption means, and said 2nd encryption means to an encryption reserve key storage means, and transmitting to said decode key storage means by using the result of said 2nd decryption means as a new decode key.
[Claim 4] the 1st counting to which said sending station carries out counting of the count of transmission -- with a means and the 1st count storage means which memorizes said count of transmission, and said count upper limit of transmission An update information storage means, and the 1st said count of transmission and said count upper limit of transmission which memorizes update information are investigated. If said count upper limit of transmission becomes below constant value, constant value will be added to said count upper limit of transmission. If said count of transmission and said count upper limit of transmission are equal, said update information will be written in said count upper limit of transmission. Updating initiation is notified and it has the 1st decision means which performs the transfer to said update information storage means of new update information after that. Said receiving station the 2nd counting which carries out counting of the count of reception -- with a means and the 2nd count storage means which memorizes said count of reception, and said count upper limit of reception If said count of reception and said count upper limit of reception are investigated and said count upper

limit of reception becomes below constant value, constant value will be added to said count upper limit of reception. Cryptocommunication equipment according to claim 1 characterized by having the 2nd decision means which will write said update information in said count upper limit of reception if said count of reception and said count upper limit of reception are equal, notifies updating initiation, and performs the transfer to said update information storage means of new update information after that.

[Translation done.]